UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/582,440	04/23/2007	Seok-Heon Cho	1403-06	6957

66547 7590 06/07/2011
THE FARRELL LAW FIRM, P.C.
290 Broadhollow Road
Suite 210E
Melville, NY 11747

EXAMINER	
SHEN, QUN	
ART UNIT	**PAPER NUMBER**
2617	
MAIL DATE	**DELIVERY MODE**
06/07/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/582,440	**Applicant(s)** CHO ET AL.	
	Examiner QUN SHEN	**Art Unit** 2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 March 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-9 and 11-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-9 and 11-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 February 2010* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This communication is a Second Action Final on the merits (RCE). Claims 2-3 and 10 are canceled. Claims 1, 6, 13, 17, and 20 are amended. Claims 1, 4-9, 11-22, after amendment, are currently pending and have been considered below.

Priority

Applicant's foreign priority claim for the benefits of KOREA 10-2003-0088895 filed on December 09, 2003 and KOREA 10-2004-0050346 filed on June 30, 2004 on the basis of 371 PCT /KR04/03212 filed on December 08, 2004, is acknowledged.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in **Graham v. John Deere Co., 383 U.S. 1, 148 USPQ 459 (1966)**, that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows: ***(See MPEP Ch. 2141)***

a. Determining the scope and contents of the prior art;
b. Ascertaining the differences between the prior art and the claims in issue;
c. Resolving the level of ordinary skill in the pertinent art; and
d. Evaluating evidence of secondary considerations for indicating obviousness or nonobviousness.

1. Claims 1, 4-9, 11-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 2004/0250069 A1, Kosamo, (hereinafter Kosamo), in view of IEEE Std 802.16-2001 (hereinafter IEEE).

As to claim 1, Kosamo discloses a method for requesting a service-specific traffic encryption key from a subscriber station to a base station in a data communication system (Fig 1: S10, par 0034, HSS, GGSN/GMSC, and a base station is a part of network, although HSS (home subscriber server) is drawn separately from base station, it can be connected to a base station or GGSN/GMSC but accessed through a base station by a subscriber station (UE)). The method comprising:

(a) determining a service type for a traffic encryption key to be used for security on a traffic connection to the base station prior to establishing the traffic connection with the base station (Fig 2, pars 0009, 0031, 0035, 0043-0045);

(b) generating a Key Request message for requesting a traffic encryption key corresponding to the determined service type, wherein the Key Request message includes the determined service type prior to establishing the traffic connection with the base station; (pars 0014, 0016-0017, traffic security/encryption parameters (encryption key is a security parameter, Figs 1-2, pars 0035-0036, 0043-0047, encryption options include service specific options, therefore the key request message for encryption would be service specific, i.e. includes the determined service type); Note that an ordinary skill in the art would appreciate that the encryption procedure would have to be completed prior to actual traffic communication (to be secured by the encryption method) start to enable a secure communication. This is also indicated in Fig 2 of Kosamo, where traffic connection (i.e. data communication S24) occurs after appropriate per service/application encryption has completed.

(d) receiving a Key Reply message including the traffic encryption key corresponding to the determined service type from the base station prior to establishing the traffic connection with the base station (Fig 2, pars 0043-0047 and discussion in (b)).

Note that Kosamo does not explicitly disclose the generated Key Request message to the base station being sent using a media access control (MAC) message prior to establishing the traffic connection with the base station, it is implied, however, in the call establishment process for a secured communication since such message is typically assembled in MAC layer. Kosamo does not elaborate in (a), wherein the traffic encryption key is used to encrypt traffic data to be transferred through a data traffic between the subscriber station and the base station, and the service type represents a type of the data traffic and is one of a unicast service, a multicast service, and a broadcast service. However, Kosamo teaches a secured data communication system for UMTS (a 3G system) which supports a unicast, a multicast, or a broadcast service (being specified in related UMTS standards). Therefore, the traffic encryption method can be applied to such services.

Nevertheless, IEEE, defines Key Request message in the over the air (OTA) protocol for SS (service subscriber), i.e. to send the message to the BS (i.e. base station) for periodically refreshing of security keying material (IEEE: Section 7.2.2). Such message is sent using a MAC message (see IEEE: section 6, Table 25, code 7) with the service type as a parameter or attribute (see IEEE: section 7.1.2-7.1.3, 7.2.2, 6.1.1.1-6.1.1.2), the data traffic services comprises a unicast service (IEEE: section 6.2.6.4.1), a multicast service, and a broadcast service (IEEE: section 6.2.6.4.2), and receiving a Key Reply message including the traffic encryption key corresponding to the determined service type from the base station_(IEEE: section 6.2.2.3.9.6 Key Reply message, also see sections 7.2.2, 7.4.1.3).

Therefore, consider Kosamo and IEEE teachings together, it would have been obvious to one of skill in the art at the time of invention to incorporate teachings in IEEE's specification discussed above in Kosamo's service specific traffic encryption method to adopt Kosamo's adaptive and selective security parameters for WiMAX wireless communication applications.

As to claim 4, Kosamo as modified discloses the method as claimed in claim 1, wherein when the service type is a multicast service, the parameter of the Key Request message includes an ID containing an identifier of a multicast service group for a subscriber (IEEE: section 6.2.6.4.2, Table 59).

As to claim 5, Kosamo as modified discloses the method as claimed in claim 1, wherein the step (c) includes sending the Key Request message using a PKM-REQ (Privacy Key Management-Request) that is one of MAC messages of the IEEE 802.16 standard protocol (IEEE: 6.2.2.3.9).

As to claim 6, claim 6 recites a method for generating and distributing a service-specific traffic encryption key from a base station to a subscriber station in a data communication system with equivalent or similar limitations to realize the features and functions in the message protocol processes between a subscriber station and a base station. Cited references also read on claim 6. Claim 6 is therefore rejected with the same reason set forth in claim 1 (see discussion and rejection above).

As to claim 7, claim 7, Kosamo as modified discloses the method as claimed in claim 6, wherein the base station analyzes the parameter to determine the service type (IEEE Sec 6.1.1.2.2, 6.2.1.3.2).

As to claim 8, Kosamo as modified discloses the method as claimed in claim 6, wherein the step (c) includes: in the case that generation of the traffic encryption key for the subscriber station is a failure due to the determined service type, the base station generating a Key Reject message including an error code indicating a reason of the failure and sending the generated Key Reject message to the subscriber station using a MAC message (Kosamo: para [0035], IEEE: 6.2.2.3.9.7).

As to claim 9, Kosamo as modified discloses the method as claimed in claim 8 but does not explicitly disclose the base station enters "unsupported service type" on the error code and sends the error code to the subscriber station in the case that the traffic encryption key for a service type corresponding to a traffic encryption key request of the subscriber station cannot be generated and distributed. However, IEEE defines Key Request message and Key Reply/Reject message between base station and mobile station and error code with respect to reason of Key Reject and also assign numerous error codes for different reasons (see IEEE: section 11.2.10, Table 132). Therefore, it would have been obvious to one of skill in the art at the time of invention to utilize messages and protocol defined in IEEE to communicate, identify and indicate traffic encryption key request of the subscriber station cannot be generated and distributed in the situation when the requested service is unsupported.

As to claim 11, Kosamo as modified discloses the method as claimed in claim 6 but does not explicitly disclose the base station enters "unauthorized multicast service group ID" on the error code and sends the error code to the subscriber station in the case that the service type for the traffic encryption key requested by the subscriber station is a multicast service and defined as unsupported multicast service for the specific multicast service group ID, because the SS is not authorized for the specific multicast service group by the base station. However, IEEE defines Key Request message and Key Reject message between base station and mobile station and error code with respect to reason of Key Reject. Therefore, it would have been obvious to one of skill in the art at the time of invention to utilize messages and protocol defined in IEEE to communicate, identify and indicate situation when the requested service is unsupported.

As to claim 12, Kosamo as modified discloses the method as claimed in claim 8, wherein the Key Reply message and the Key Reject message are sent using a PKM-RSP (Privacy Key Management-Response) message that is one of MAC messages of the IEEE 802.16 standard protocol (IEEE: Section 6.2.2.3.9).

As to claim 13, claim 13 recites protocol configuration method that necessitates the method claims 1 and 6. Rejections on claims 1 and 6 are therefore incorporated herein (see analysis and rejections above).

As to claims 14 and 15, they are rejected with the same reason set forth in claims 5 and 8, respectively.

As to claim 16, Kosamo as modified discloses the protocol configuration method as claimed in claim 15, wherein the step (b) comprises: sending the Key Reply message and the Key Reject message using a PKM-RSP message that is one of MAC messages of the IEEE 802.16 standard protocol (IEEE: section 6.2.2.3.9).

As to claim 17, claim 17 recites an apparatus claim for the apparatus wirelessly connected to a base station in a data communication system so as to request a service-specific traffic encryption key from the base station, comprising a Key Request message generator, a Key Request message sender, a Key Reply/Reject message receiver, a message analyzer, and a key request controller. The apparatus encompasses and necessitates method claims 1, 6 and 13. Rejections on claims 1, 6 and 13 are therefore incorporated herein.

As to claim 18, claim 18 is rejected on the same ground as claim 4. The apparatus as claimed in claim 17, wherein the Key Request message further comprises a multicast service group ID of the subscriber station when the service type is a multicast service (IEEE: section 6.2.12).

As to claim 19, Kosamo as modified discloses the apparatus as claimed in claim 17, further comprising: a memory for storing information including the traffic encryption key or the error code resulted from an analysis of the message analyzer under the control of the key request controller (Kosamo: pars 0011 0014, 0024, 0033, 0035, 0039).

As to claim 20, claim 20 recites an apparatus claim for the apparatus provided to a base station for generating and distributing a service-specific traffic encryption key in a <u>data communication</u> system, which encompasses and necessitates method claims 1, 6 and 13. Rejections on claims 1, 6 and 13 are therefore incorporated herein (see analysis and rejection on claims 1, 6 and 13).

As to claim 21, Kosamo as modified discloses the apparatus as claimed in claim 20, further comprising: a Key Reject message sender for sending a Key Reject message including an error code to the subscriber station using a MAC message under the control of the key generation and distribution controller in the case that the traffic encryption key generator generates an error for the request of the subscriber station (see IEEE: section 6.2.2.3.9.7).

As to claim 22, Kosamo as modified discloses the apparatus as claimed in claim 20, further comprising a memory for storing information including an analysis result of the message analyzer and a discrimination result of the subscriber discriminator under the control of the key generation and distribution controller (see rejection in claim 19).

Response to Argument

Applicant's arguments filed on August 20, 2010 have been fully considered but they are not persuasive. Applicant essentially argues that the further amended feature of completing the service specific encryption process (including all necessary steps of message exchange) prior to establishing the traffic connection with the base station (in claims 1, and other independent claims) would overcome prior arts of record. As indicated in the office action, such feature is necessitated in order to enable a secure communication as understood by an ordinary skill in the art and also indicated by Kosamo (Fig 2, pars 0043-0047).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to QUN SHEN whose telephone number is (571)270-7927. The examiner can normally be reached on 9:30 am - 6:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jinsong Hu can be reached on 571-272-3965. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/QUN SHEN/
Examiner, Art Unit 2617

/Jinsong Hu/
Supervisory Patent Examiner,
Art Unit 2617